Генеральная прокуратура Российской Федерации

УПОЛНОМОЧЕННЫЙ РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИ ЕВРОПЕЙСКОМ СУДЕ ПО ПРАВАМ ЧЕЛОВЕКА

General Prosecutor's Office
of the Russian Federation

**Representative
of the Russian Federation
at the European Court of Human Rights**

Office du Procureur Général
de la Fédération de Russie

**Représentant
de la Fédération de Russie auprès de
la Cour Européenne des Droits de l'Homme**

Bolshaya Dmitrovka str., 15A, build. 1, Moscow, 125993

e-mail: rusrepr@genproc.gov.ru

15 November 2021 № Исорг-35-8111-21/177330

Mrs Olga Chernishova
Deputy Section Registrar
Third Section

European Court
of Human Rights

Application no. 33696/19
Podchasov v. Russia

Dear Madame,

With reference to your letter of 24 June 2021 in respect of the above application please find attached a copy of the Memorandum of the authorities of the Russian Federation.

As regards the English translation of the Memorandum, it will be forwarded to you in due course.

Yours faithfully,

Mikhail Vinogradov

Генеральная прокуратура Российской Федерации
№ Исорг-35-8111-21/177330

Генеральная прокуратура Российской Федерации

УПОЛНОМОЧЕННЫЙ РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИ ЕВРОПЕЙСКОМ СУДЕ ПО ПРАВАМ ЧЕЛОВЕКА

General Prosecutor's Office
of the Russian Federation

**Representative
of the Russian Federation
at the European Court of Human Rights**

Office du Procureur Général
de la Fédération de Russie

**Représentant
de la Fédération de Russie auprès de
la Cour Européenne des Droits de l'Homme**

Bolshaya Dmitrovka str., 15A, build. 1, Moscow, 125993

e-mail: rusrepr@genproc.gov.ru

15 November 2021 № Исорг-35-8111-21/177330

**ЕВРОПЕЙСКИЙ СУД
ПО ПРАВАМ ЧЕЛОВЕКА**

**МЕМОРАНДУМ
по жалобе № 33696/19
«Подчасов против Российской Федерации»**

1. 24 июня 2021 г. Европейский Суд по правам человека сообщил властям Российской Федерации о жалобе № 33696/19 «Подчасов против Российской Федерации», поданной в соответствии со статьей 34 Конвенции о защите прав человека и основных свобод гражданином Российской Федерации Подчасовым Антоном Валерьевичем.

2. Европейский Суд в соответствии с подпунктом «b» пункта 2 правила 54 Регламента предложил властям Российской Федерации представить свои замечания и ответить на следующие вопросы:

«1. Имело ли место нарушение права заявителя на уважение его частной жизни и корреспонденции, гарантированного статьей 8 Конвенции, в результате самого факта существования спорного законодательства (см. постановление Большой Палаты Европейского Суда «Роман Захаров против Российской Федерации», жалоба № 47143/06, ECHR 2015, §§ 170-179)? Отвечает ли спорное законодательство требованию «качества закона», предусматривая наличие адекватных и эффективных гарантий против произвола и риска злоупотребления? Неспособно ли оно сдерживать «вмешательство» в той степени, которая «необходима в демократическом обществе»?

2. Учитывая выводы судов о том, что запрос ФСБ России, адресованный Telegram Messenger LLP, не затрагивал прав заявителя, имел ли он в своем распоряжении эффективные средства правовой защиты в отношении его жалобы в соответствии со статьей 8 Конвенции, как того требует статья 13 Конвенции?»

Обстоятельства дела

3. Власти Российской Федерации согласны с хронологией событий, изложенной заявителем, но не согласны с его доводами. Таким образом, изложение позиции государства будет содержаться в ответах на вопросы, поставленные Европейским Судом.

Ответ на вопрос № 1

4. Власти Российской Федерации полагают, что в настоящем деле отсутствовало вмешательство в права заявителя, и жалоба заявителя является явно необоснованной. Однако, если Европейский Суд все же придет к выводу о наличии вмешательства государства в осуществление прав заявителя, предусмотренных пунктом 1 статьи 8 Конвенции, власти Российской Федерации утверждают, что предполагаемое вмешательство было предусмотрено соответствующим национальным законом, уровень доступности и предсказуемости которого был достаточно высок, чтобы удовлетворять требованию «качества закона», вытекающему из прецедентной практики Европейского Суда, преследовало законную цель и было необходимо в демократическом обществе для достижения этой цели.

а) Вмешательство было основано на законе

5. В июле 2016 г. в Российской Федерации был принят ряд законов, имеющих антитеррористическую направленность.

6. Так, Федеральным законом от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности» были внесены изменения в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и другие федеральные законы.

7. В связи с изменениями пункт 3 статьи 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации» был изложен в следующей редакции: «Организатор распространения информации в сети «Интернет» обязан хранить на

территории Российской Федерации:

1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети «Интернет» и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий;

2) текстовые сообщения пользователей сети «Интернет», голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети «Интернет» до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Порядок, сроки и объем хранения указанной в настоящем подпункте информации устанавливаются Правительством Российской Федерации.

8. Кроме того, статья 10.1 была дополнена пунктами 3.1. и 4.1. В соответствии с пунктом 3.1. Организатор распространения информации в сети «Интернет» (далее – ОРИ) обязан предоставлять указанную выше информацию уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами. Согласно пункту 4.1. при использовании для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет» дополнительного кодирования электронных сообщений и (или) при предоставлении пользователям сети «Интернет» возможности дополнительного кодирования электронных сообщений ОРИ обязан представлять в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений.

9. В целях реализации положений статьи 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации» 19 июля 2016 г. ФСБ России был издан Приказ № 432 «Об утверждении Порядка представления ОРИ в Федеральную службу безопасности Российской Федерации информации, необходимой для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет» (далее – Порядок).

10. Согласно пункту 3 Порядка ОРИ осуществляет передачу информации для декодирования на основании запроса уполномоченного подразделения, подписанного начальником (заместителем начальника) уполномоченного подразделения, в возможно короткий срок, но не более 10 дней со дня получения запроса.

b) Вмешательство основано на положениях национального законодательства, которые являются достаточно ясными, доступными и предсказуемыми в их формулировке и толковании

11. Согласно прецедентной практике Европейского Суда выражение «предусмотрено законом» не только требует, чтобы оспариваемая по делу мера была предусмотрена соответствующим национальным законом, но и относилась к качеству этого закона: он должен быть доступен тем лицам, которых он касается, и предсказуем в отношении последствий его применения. Закон, о котором идет речь, должен соответствовать принципу верховенства права, а значит, предоставлять меру правовой защиты от произвольного вмешательства органов государственной власти в реализацию прав, предусмотренных пунктом 1 статьи 8 Конвенции. В случаях негласного осуществления полномочий исполнительной власти риск произвола особенно очевиден. Поскольку принятие мер негласного наблюдения не контролируется лицами, за которыми это наблюдение ведется, или обществом в целом, предоставление органам исполнительной власти юридической свободы действий путем наделения их неограниченными полномочиями противоречило бы принципу верховенства права. Следовательно, закон должен указывать границы любой такой свободы действий, которой наделяются компетентные органы власти, и способы ее осуществления с достаточной четкостью, с учетом правомерной цели тех мер, о которых идет речь для того, чтобы предоставить человеку адекватную защиту от произвольного вмешательства государства в реализацию его прав (постановление Европейского Суда по делу «Segerstedt -Wiberg and others v. Sweden» от 6 июня 2006 г., жалоба № 62332/00, § 76).

12. Что касается доступности перечисленных выше правовых норм власти Российской Федерации отмечают, что они были официально опубликованы и находились в свободном доступе, в том числе в сети Интернет, и были доступны общественности.

13. Что касается предсказуемости данных правовых норм, то согласно прецедентной практике Европейского Суда национальное законодательство должно определить сферу применения мер скрытого наблюдения, давая гражданам адекватное представление об обстоятельствах, при которых органы государственной власти имеют право прибегать к таким мерам, в частности, путем четкого изложения характера правонарушений, которые могут привести к санкционированию прослушивания и определения категорий лиц, телефоны которых подлежат прослушиванию (постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации», от 4 декабря 2015 г., жалоба № 47143/06, § 243; решение

Европейского Суда о неприемлемости жалобы «Weber and Saravia v. Germany» от 10 января 2020 г., жалоба № 54934/00, § 93).

14. В связи с этим власти Российской Федерации отмечают, что в статье 8 Федерального закона от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» законодателем указано, что проведение оперативно-разыскных мероприятий, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи, а также право на неприкосновенность жилища, допускается на основании судебного решения и при наличии информации: о признаках подготавливаемого, совершаемого или совершенного противоправного деяния, по которому производство предварительного следствия обязательно; о лицах, подготавливающих, совершающих или совершивших противоправное деяние, по которому производство предварительного следствия обязательно; о событиях или действиях (бездействии), создающих угрозу государственной, военной, экономической, информационной или экологической безопасности Российской Федерации.

15. Согласно той же статьи прослушивание телефонных и иных переговоров допускается только в отношении лиц, подозреваемых или обвиняемых в совершении преступлений средней тяжести, тяжких или особо тяжких преступлений, а также лиц, которые могут располагать сведениями об указанных преступлениях. Фонограммы, полученные в результате прослушивания телефонных и иных переговоров, хранятся в опечатанном виде в условиях, исключающих возможность их прослушивания и тиражирования посторонними лицами.

16. При этом предоставление ОРИ ключей шифрования органам безопасности не означает, что полученная ФСБ России информация, позволяющая декодировать электронные сообщения, будет доступна неограниченному числу сотрудников органов ФСБ России, а соответствующими руководителями не созданы условия для выполнения сотрудниками своих должностных (функциональных) обязанностей лишь в тех объемах и пределах, которые для этого необходимы. В любом случае для должностных лиц, осуществляющих оперативно-разыскную деятельность, установлен запрет на разглашение сведений, которые затрагивают неприкосновенность частной жизни, личную и семейную тайну, честь и доброе имя граждан и которые стали известными в процессе проведения оперативно-разыскного мероприятия, нарушение которого влечет ответственность, установленную законодательством Российской Федерации.

17. Сведения, составляющие тайну переписки, сообщений, могут быть получены в рамках оперативно-разыскного мероприятия, которые проводятся на основании судебного решения, выдаваемого органу – инициатору проведения оперативно-разыскного мероприятия лишь при

наличии оснований для его проведения (статья 9 Федерального закона «Об оперативно-розыскной деятельности»). Очевидно, что санкционированный судом доступ к информации, составляющей тайну переписки, сообщений, предполагает ознакомление уполномоченных лиц с содержимым самих сообщений, а соответственно, конституционное право гражданина ограничивается в ходе проведенного оперативно-разыскного мероприятия, а не в результате представления ОРИ ключевого материала, цель получения которого - использование уполномоченным органом уже полученных с разрешения суда защищаемых законом сведений. Таким образом, по смыслу Федерального закона «Об оперативно-розыскной деятельности» потребность в декодировании информации, полученной в результате проведенных с санкции суда оперативно-разыскных мероприятий, сама по себе не предопределяет необходимость вынесения об этом специального судебного решения, в связи с чем такое решение, в принципе, не может быть предоставлено ОРИ при направлении органом безопасности соответствующего запроса.

18. Кроме того, Верховным Судом Российской Федерации 20 марта 2018 г. и 9 августа 2018 г. в решении и апелляционном определении по рассматриваемому вопросу отмечено, что положения приказа ФСБ России не содержат требований о передаче ФСБ России электронных сообщений и информации о факте их приема-передачи, то есть информации, составляющей тайну переписки.

19. Таким образом, власти Российской Федерации полагают, что российское законодательство предоставляет достаточные процессуальные гарантии против злоупотребления полномочиями по проведению оперативно-разыскных мероприятий, ограничивающих конституционные права граждан и дает адекватное указание на обстоятельства и условия, при которых государственные органы имеют право прибегать к таким мерам и условия, при которых граждане могут ожидать, что могут подвергнуться таким мерам.

c) Вмешательство было необходимо в демократическом обществе и преследовало «острую социальную необходимость»

20. Европейский Суд признаёт, что органы, осуществляющие оперативно-разыскную деятельность, могут на законных основаниях существовать в демократическом обществе. Тем не менее, Европейский Суд вновь отмечает, что осуществление полномочий по негласному наблюдению за гражданами приемлемо с точки зрения Конвенции лишь постольку, поскольку оно строго необходимо для охраны демократических институтов (см. постановление Европейского Суда по делу «Класс и другие заявители против Германии» от 6 сентября 1978 г., жалоба № 5029/71, § 42; а также постановление Большой Палаты

Европейского Суда по делу «Ротару против Румынии», § 47). Такого рода вмешательство государства в осуществление гражданами своих прав должно быть подкреплено соответствующими и достаточными основаниями и быть соразмерным преследуемой государством правомерной цели или целям. В связи с этим Суд полагает, что национальные власти обладают свободой усмотрения, объем которой зависит не только от характера преследуемой ими правомерной цели, но и от характера конкретного вмешательства, имевшего место в том или ином случае. В настоящем деле следует найти равновесие между интересом государства-ответчика в охране национальной безопасности и в борьбе с терроризмом, с одной стороны, и серьезностью вмешательства государства в реализацию права заявителей на уважение их личной жизни, с другой стороны («Segerstedt -Wiberg and Others v. Sweden», § 88).

21. Власти Российской Федерации утверждают, что предполагаемое вмешательство в связи с существованием самого спорного законодательства было «необходимым в демократическом обществе» и преследовало «острую социальную необходимость» в целях национальной безопасности. Для этого органам службы безопасности требуются инструменты для своевременного и эффективного обнаружения угроз, возникающих в цифровом пространстве. Несомненно, одним из таких инструментов является перехват информации. Многие из этих угроз исходят от международных сетей враждебных субъектов, имеющих доступ ко все более совершенным технологиям, позволяющим им остаться незамеченными. Доступ к такой технологии также позволяет враждебным государственным и негосударственным субъектам нарушать цифровую инфраструктуру и даже надлежащее функционирование демократических процессов с помощью кибератак, что представляет собой серьезную угрозу национальной безопасности, которая по определению существует только в цифровой сфере и как таковая может быть обнаружена и исследована только там (постановление Большой Палаты Европейского Суда по делу «Big Brother Watch and Others v. the United Kingdom» от 25 мая 2021 г., жалобы №№ 58170/13, 62322/14 и 24960/15, § 323).

22. Так, например, в декабре 2017 г. ФСБ России был предотвращен теракт «в одном из культовых учреждений» Санкт-Петербурга, было задержано 7 членов террористической организации. В открытых источниках сообщалось, что руководство ячейкой осуществлялось главарями международной террористической организации и-за рубежа посредством интернет-мессенджера Telegram. В апреле 2017 г. в метро Санкт-Петербурга произошел теракт, в результате которого погибли 15 человек и около 100 пострадали. По сведениям ФСБ России, террористами руководили через мессенджер Telegram, предоставляющий террористам возможность создавать

секретные чаты с высоким уровнем шифрования передаваемой информации.

23. Кроме того, Европейский Суд ранее устанавливал, что требование «предсказуемости» закона не обязывает государства принять правовые положения, подробно перечисляющие все виды действий, которые могут привести к решению о скрытом наблюдении по основаниям «национальной безопасности». По своей природе угрозы национальной безопасности могут различаться по характеру и быть неожиданными или трудно определяемыми заранее (см. выше Постановление Европейского Суда по делу «Kennedy v. the United Kingdom» от 18 мая 2010 г., жалоба № 26839/05, § 159). Вместе с тем Европейский Суд напоминает, что в вопросах, затрагивающих основные права, противоречило бы принципу верховенства права, одному из основных принципов демократического общества, воплощенных в Конвенции, если бы исполнительная власть пользовалась дискрецией в степени неограниченных юридических полномочий. Соответственно, закон должен с достаточной ясностью указывать пределы любого такого усмотрения, предоставленного компетентным органам, и способ его реализации с учетом законной цели данной меры с тем, чтобы предоставить человеку соответствующую защиту от произвольного вмешательства

24. В своей прецедентной практике о мерах скрытого наблюдения Европейский Суд разработал следующие минимальные гарантии, которые должны быть установлены в законе для того, чтобы избежать превышение полномочий властью о характере правонарушений, которые могут инициировать санкцию на прослушивание, определение категорий лиц, телефоны которых подлежат прослушиванию, ограничение на продолжительность телефонного прослушивания, порядок изучения, использования и хранения полученных данных, о мерах предосторожности при передаче данных другим лицам, и обстоятельства, при которых записи могут или должны быть стерты или уничтожены («постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации», § 231).

25. Что касается вопроса, является ли вмешательство «необходимым в демократическом обществе» для достижения законной цели, Европейский Суд признал, что, выбирая между заинтересованностью государства-ответчика в деле защиты своей национальной безопасности посредством мер скрытого наблюдения и серьезностью вмешательства в права заявителя на уважение его личной жизни, внутригосударственные власти пользуются определенной свободой усмотрения в выборе средств для достижения законной цели защиты национальной безопасности. Однако эти границы могут регулироваться в ходе надзора, который охватывает как законодательство, так и решения, применяемые на его основе. Ввиду

риска того, что система скрытого наблюдения с целью защиты национальной безопасности может умалять или даже уничтожить демократические ценности под предлогом их защиты, Европейскому Суду должно быть продемонстрировано существование адекватных и эффективных гарантий против превышения полномочий. Оценка зависит от всех обстоятельств дела, таких как характер, объем и продолжительность возможных мер, оснований, необходимых для их санкционирования, компетентные органы, правомочные разрешить, провести и проконтролировать их, и вид правовой защиты, предоставляемой внутригосударственным законодательством. Европейский Суд должен определить, будет ли порядок надзора за санкционированием и осуществлением ограничительных мер достаточным, чтобы «вмешательство» оставалось в рамках того, что является «необходимым в демократическом обществе» (постановление Большой Палаты Европейского Суда по делу «Роман Захаров против Российской Федерации», § 232).

26. Власти Российской Федерации полагают, что в Российской Федерации приняты все надлежащие меры предосторожности для изучения, использования, хранения и уничтожения полученных в рамках оперативно-разыскных мероприятий материалов и настаивают в связи с этим на отсутствии нарушения права заявителя на уважение частной жизни и корреспонденции.

27. Европейский Суд ранее приходил к выводу, что, хотя существование режима наблюдения может являться вмешательством в частную жизнь, жалобы на то, что это нарушало права, подлежат рассмотрению в судебном порядке только в случаях, где существует «разумная вероятность», что лицо являлось на самом деле жертвой незаконного наблюдения (см. Решение Комиссии по правам человека по делу «Esbester v. United Kingdom» от 2 апреля 1993 г., жалоба № 18601/91).

28. В связи с этим власти Российской Федерации отмечают, что заявитель может претендовать на роль жертвы только в том случае, если он сможет доказать существование «разумной вероятности» того, что органы безопасности осуществляли сбор касающихся его персональных данных и, следовательно, допустили вмешательство в его личную жизнь.

29. Однако, заявитель не представил доказательств того, что представляет интерес для органов службы безопасности.

30. Относительно довода заявителя о том, что действия ФСБ России, заключающиеся в требовании от Telegram Messenger LLP предоставить информацию, позволяющую декодировать сообщения всех пользователей Telegram, власти Российской Федерации выражают несогласие и отмечают, что Приказом № 432 ФСБ России установила общую обязанность ОРИ предоставлять ключи шифрования, однако требования передавать спецслужбам ключи расшифровки всего трафика в

приказе не содержится. Более того, власти Российской Федерации отмечают, что обязанность ОРИ предоставления таких сведений возможна только по запросу, в котором запрашиваемые сведения конкретизируются.

31. Так, вопреки доводам заявителя о возможности декодирования сообщений всех пользователей, в оспариваемом заявителем запросе ФСБ России от 12 июля 2017 г., адресованном в Telegram Messenger LLP, следует, что органами безопасности была запрошена информация, необходимая для декодирования сообщений пользователей интернет-мессенджера Telegram по 6 телефонным номерам (что также указано в постановлении по делу об административном правонарушении Мещанского районного суда г. Москвы от 16 октября 2017 г.). Кроме того, согласно указанному запросу данные лица подозревались в причастности к террористической деятельности, что по российскому законодательству является особо тяжким преступлением. Более того, в запросе ФСБ России был указан номер судебной санкции, т.е. проведение данного оперативно-разыскного мероприятия было санкционировано судом.

32. Таким образом доводы заявителя о нарушении Приказом ФСБ России № 432 его частной жизни, а также о полном доступе органов безопасности к переписке пользователей являются необоснованными.

33. Учитывая изложенное, власти Российской Федерации полагают, что нарушения права заявителя на уважение его частной жизни и корреспонденции, гарантированного статьей 8 Конвенции, в результате самого факта существования спорного законодательства не имело места, а спорное законодательство отвечает требованию «качества закона», предусматривая наличие адекватных и эффективных гарантий против произвола и риска злоупотребления.

Ответ на вопрос № 2

34. Отвечая на второй вопрос Европейского Суда, власти Российской Федерации сообщают, что в распоряжении заявителя имелись эффективные средства правовой защиты в отношении его жалобы в соответствии со статьей 8 Конвенции, как того требует статья 13 Конвенции. Более того, заявитель воспользовался ими.

35. Однако, тот факт, что национальные суды пришли к выводу о том, что обжалуемые действия не нарушали либо иным образом не затрагивали права, свободы и законные интересы истца, и отказали на этом основании заявителю в принятии административного искового заявления не свидетельствует об отсутствии в распоряжении заявителя эффективных средств правовой защиты.

36. Власти Российской Федерации, таким образом, поддерживают свой довод о том, что заявитель не представил доказательств того, что

имелась «разумная вероятность» того, что он представляет интерес для органов службы безопасности.

37. «Комиссия напоминает, что статья 13 Конвенции не требует средств правовой защиты в соответствии с национальным законодательством в отношении любого предполагаемого нарушения Конвенции. Это применимо только в том случае, если можно сказать, что у лица есть «аргументированная жалоба» о нарушении Конвенции. Комиссия считает, что в свете вышеприведенных выводов нельзя утверждать, что заявитель имеет «аргументированное требование» о нарушении его прав, предусмотренных Конвенцией. Следовательно, данная жалоба должна быть отклонена как явно необоснованная по смыслу пункта 2 статьи 27 Конвенции» (см. цитированное выше Решение Комиссии по правам человека по делу «Esbester v. United Kingdom»).

38. Учитывая изложенное, власти Российской Федерации полагают, что в настоящем деле отсутствовало нарушение статьи 13 Конвенции.

I. Законодательство и практика получения спецслужбами государств-участников Совета Европы сведений у ОРИ

39. Власти Российской Федерации хотели бы обратить внимание на то, что в странах Совета Европы существует аналогичная практика получения органами безопасности сведений у ОРИ и попыток ограничить сквозное шифрование переписки пользователей различных мессенджеров. В связи с этим хотели бы привести выдержки из законодательства некоторых стран-участниц Совета Европы, регулирующего данную сферу отношений.

Великобритания:

40. С 29 ноября 2016 г. в Великобритании действует Закон «О следственных полномочиях» (Investigatory Powers Act), известный также как «Шпионский устав» (Snooper's Charter), который дает возможность широкому кругу британских органов власти под предлогом борьбы с терроризмом получать доступ к пользовательским данным своих граждан и обязывает операторов связи хранить метаданные обо всех коммуникациях своих клиентов в течение 1 года. «Шпионский устав» регулирует порядок доступа уполномоченных органов к данным о коммуникациях в рамках следственных действий по уголовным делам, санкции по которым предусматривают тюремное заключение сроком не менее 6 месяцев (т.е. по «серьезным преступлениям»). При этом речь может идти о взломе компьютеров, мобильных телефонов, серверов, включая внедрение программного обеспечения, позволяющего отслеживать все данные, вводимые через клавиатуру. Закон определяет

довольно широкий круг уполномоченных ведомств и должностных лиц, имеющих право на доступ к данным о коммуникациях. Помимо правоохранительных органов и спецслужб к ним относятся, например, министерства транспорта, здравоохранения, труда и пенсионного обеспечения, агентство по продовольственным стандартам, таможенная служба, комиссия по контролю за азартными играми и т.д.

41. В соответствии с установленным порядком доступ к данным предоставляется на основании ордера, выдаваемого специально введенными должностными лицами: комиссар по следственным полномочиям и судебный комиссар. Они вправе также осуществлять публичный контроль за соблюдением законодательства в данной области и рассматривать случаи его нарушений.

42. Закон обязывает операторов связи собирать данные о коммуникациях своих клиентов (Internet connection records), хранить их в течение 1 года и предоставлять к ним доступ уполномоченным органам в расшифрованном виде. Последнее делает все механизмы конечного шифрования открытыми для запрашивающих органов.

43. Кроме того, властям Российской Федерации известно, что параллельно с законодательным оформлением доступа правоохранительных органов и спецслужб к пользовательским данным британские власти последовательно борются и со сквозным шифрованием в мессенджерах и соцсетях, фактически переведя технологические компании в режим осажденной крепости. До недавнего времени основная ставка делалась на попытки продавить их под предлогом борьбы с терроризмом по следам громких террористических атак («Шарли Эбдо» в 2015 году, теракт в Манчестере в 2017 году, нападения с холодным оружием в 2019 году, убийство депутата Эмесса Д. в октябре 2021 г.). Однако эта риторика пока не нашла достаточно последователей среди населения и законотворцев, поэтому власти выработали другой подход к «урегулированию интернета». Министр МВД с 2019 года Пател П. развернула кампанию против сексуального насилия над детьми и обвинила мессенджеры со сквозным шифрованием едва ли не в пособничестве в сокрытии этих преступлений. Уже разработан законопроект, ограничивающий интернет-сервисы вне зависимости от их юрисдикции в возможности защиты пользовательских данных. В частности, на них будут возложены обязательства предпринимать меры по обеспечению безопасности пользователей вплоть до запрета сквозного шифрования, а в случае нарушения требований предусмотрены штрафы до 10% от объема оборота соответствующих компаний, санкции для их руководства и возможность блокировки сервисов. При этом блокировки планируют осуществлять посредством уведомлений VPN-провайдеров. Кроме того, эксперты высказывают опасения, что власти обяжут интернет-сервисы хранить молчание относительно фактов запросов доступа со стороны уполномоченных органов.

Нидерланды:

44. Проблематика получения спецслужбами сведений, необходимых для выполнения своих функций, в том числе для защиты безопасности государства, общественной безопасности и других целей, регулируется, в первую очередь, Законом о спецслужбах и Законом о расследованиях в связи с угрозой безопасности.

45. В частности, Закон о спецслужбах регулирует задачу, цель и полномочия общей и военной служб разведки и безопасности (AIVD и MIVD). Данные службы могут использовать свои полномочия в случае, если они отвечают требованиям пропорциональности, субсидиарности и необходимости, а также если их использование является «целенаправленным». Одной из функций AIVD является «следственный перехват, ориентированный на миссию», который означает, что следователи могут перехватывать определенные сообщения из радиоволн и интернет-кабелей для дальнейшего расследования, если ситуация касается угрозы для национальной безопасности.

46. В упомянутом нормативно-правовом акте прописаны отдельные гарантии защиты частной жизни, общий стандарт хранения информации и требования к точности, полноте данных и качеству их обработки. При этом сведения, касающиеся источника журналиста, и данные, относящиеся к конфиденциальному общению между адвокатом и клиентом, могут собираться и храниться только с разрешения Гаагского окружного суда.

47. Тем не менее, несмотря на определенные гарантии, прописанные в законодательстве, данная сфера деятельности спецслужб вызывает немало нареканий со стороны экспертов и местного гражданского общества. Из-за внесенных в 2017 году поправок в законодательство возможности разведки в плане слежки были существенно расширены, в частности, узаконены полномочия разведывательных служб и служб безопасности по осуществлению тотальной слежки и прослушивания, а также перехвата сообщений не обозначенных конкретно категорий лиц.

48. Официальная статистика свидетельствует о том, что ежегодно для обеспечения национальной безопасности и борьбы с преступностью в Нидерландах совершаются тысячи подключений к телефонным сетям в целях прослушивания, зафиксировано увеличение случаев IP-прослушки через интернет.

49. В конце 2020 г. из расследования газеты «НРЦ Ханделсблад» стало известно о незаконном сборе данных граждан Центром информационных маневров (LIMC) Министерства обороны Нидерландов. Целью наблюдения подразделения стали лица, скептически настроенные к мерам правительства по сдерживанию коронавирусной инфекции, а также представители голландского отделения «желтых жилетов». Позже,

в мае 2021 г. представитель Минобороны Бейлевелд А. принесла за это извинение.

50. В апреле 2021 г. вскрылось, что Национальный координатор по борьбе с терроризмом и обеспечению безопасности (NCTV) также на протяжении нескольких лет незаконно собирал информацию о гражданах (с помощью фейковых аккаунтов). Подготовленными досье подразделение Министерства юстиции и безопасности делилось с руководством голландских муниципалитетов, Национальной полицией, Общей службой разведки и безопасности (AIVD), а также с иностранными спецслужбами. В начале июня 2021 г. газета «Фолкскрант» сообщила, что голландские муниципалитеты также использовали фейковые аккаунты для осуществления сбора информации о гражданах.

51. В настоящее время Кабинет министров Нидерландов изучает возможность ослабить защиту сообщений в чатах и ограничить сквозное шифрование чат-приложений, чтобы облегчить спецслужбам доступ к переписке. Прежде всего, речь идет о таких сервисах, как «WhatsApp» и «Facebook Messenger». Телефонные и интернет-провайдеры уже обязаны предоставлять доступ по запросу компетентных ведомств. Аналогичные меры по упрощению доступа к услугам чат-приложений в настоящее время разрабатываются Министерством юстиции с целью возможной выработки соответствующего законопроекта.

Франция:

52. Законодательство Французской Республики в области контроля над электронными коммуникациями претерпело значительные изменения в период между 2015 и 2021 годами. Во многом это было обусловлено необходимостью расширения полномочий правоохранительных органов в сфере борьбы с терроризмом. Так, обязанности операторов связи предоставлять данные государственным органам прописаны в Кодексе почтовых и электронных коммуникаций, Законе от 21 июня 2004 г. № 2004-575 «О мерах доверия в цифровой экономике», Законе от 23 января 2006 г. № 2006-64 «О борьбе с терроризмом».

53. Закон от 24 июля 2015 г. № 2015-912 «О деятельности спецслужб» значительно расширил полномочия силовых ведомств в области контроля над электронными коммуникациями. Он устранил имевшиеся в правовой области пробелы, создав универсальные юридические рамки для деятельности спецслужб и предоставил им современный комплексный инструментарий для эффективной работы, адекватный уровню новых вызовов и угроз. Компетентные ведомства официально получили право применять широкий спектр высокотехнологичных средств и техник доступа – открытого и тайного –

к различным массивам данных, в том числе и персональных, а также перехвата информации, содержания телекоммуникаций, метаданных.

54. Ведомствам разрешили использовать на национальной территории и за ее пределами оборудование и программное обеспечение, позволяющее считывать логины, пароли, уникальные технические данные, вести скрытую фотосъемку и наблюдение (в том числе посредством геолокализации); перехватывать и сохранять содержание электронной переписки и телефонных разговоров; устанавливать необходимые устройства и программы по месту проживания, внутри личного транспорта и на частной собственности объекта наблюдения.

55. Закон от 24 июля 2015 г. № 2015-912 «О деятельности спецслужб» также закрепил право спецслужб потребовать от операторов телекоммуникаций и провайдеров Интернет-связи «незамедлительного предоставления» данных об интересующих силовиков лицах и метаданных по их контактам, а также содержания их телекоммуникаций. Дешифровка коммуникаций при этом возлагается на операторов, услугами которых пользуются заинтересовавшие силовиков лица. Кроме того, предусмотрена возможность при наличии разрешения главы правительства и без разрешения судебной инстанции обязать операторов, провайдеров компании, предоставляющих услуги в Интернете или управляющих социальными сетями, «самостоятельно отслеживать» посредством автоматизированной обработки данных подозрительную активность их клиентов на основании составленных для них инструкций и сообщать результаты спецслужбам.

56. Компании, оказывающие услуги связи, должны записывать и хранить в течение одного года с момента записи следующие категории данных: информацию, позволяющую идентифицировать пользователей и адресатов коммуникаций; сведения о задействованных конечных устройствах и оборудовании; технические характеристики и метаданные; сведения о запрошенных или использованных пользователями дополнительных услугах и поставщиках этих услуг; в случае телефонной связи – еще и информацию, позволяющую идентифицировать происхождение и геолокацию коммуникации.

II. Международные документы

Конвенция о защите физических лиц при автоматизированной обработке персональных данных

57. Статья 9 указанной Конвенции (сторонами которой являются все государства-члены Совета Европы) напрямую предусматривает возможность отступления от ее положений в интересах «защиты безопасности государства, общественной безопасности, валютно-

кредитных интересов государства или пресечения уголовных преступлений».

Сравнительный анализ законодательства государств-участников Конвенции в сфере получения доступа госорганов к данным об абонентах, подготовленный в рамках Комитета Конвенции о преступности в сфере компьютерной информации

58. В соответствии с указанным документом эффективные решения по вопросу получения данных об абонентах уже несколько лет находятся в центре внимания Комитета Конвенции о преступности в сфере компьютерной информации, учитывая важность такой информации для расследования преступлений (далее – Комитет).

59. В 2014 году Комитет провел опрос на тему «Правил получения данных об абонентах» и в 2017 году принял «Руководство по распоряжению о предъявлении данных об абонентах» в соответствии со статьей 18 Конвенции о компьютерных преступлениях.

60. Что касается предварительных решений Суда Справедливости Европейского Союза по вопросу хранения данных 2014 и 2016 годов, то они не касаются конкретно данных об абонентах. Однако, они тем не менее важны, в связи с тем, что:

- Директива ЕС № 2006/21/ЕС требует сохранения ряда категорий данных, включая IP-адреса, относящиеся к абонентам, и, соответственно, правила доступа к сведениям об абонентах в государствах-членах Европейского Союза могут быть идентичны правилам доступа к данным о трафике;
- общее сохранение различных категорий данных «в целом» считается несоразмерным. Сохранение или доступ в ходе расследования конкретных уголовных дел к более ограниченной категории данных, таких как данные об абонентах, не может подпадать под строгие ограничения, установленные Судом Справедливости Европейского Союза.

61. Таким образом, из представленного следует, что законодательство стран-участниц Совета Европы, законодательство Европейского Союза, а также практика перехвата информации спецслужбами в данных государствах существует повсеместно, однако, по мнению властей Российской Федерации, к ответственности привлекаются только страны с так называемой «неокрепшей демократией», к которой очевидно относят и Российскую Федерацию.

ВЫВОДЫ И ТРЕБОВАНИЯ

На основании изложенного, представляя интересы Российской Федерации в соответствии со статьями 39^1 и 39^2 Федерального закона «О прокуратуре Российской Федерации» и Указом Президента Российской Федерации от 8 июля 2021 г. № 412 «Об Уполномоченном Российской Федерации при Европейском Суде по правам человека»,

ПОЛАГАЮ:

жалоба Подчасова А.В. на предполагаемое нарушение его прав, гарантированных статьей 8 Конвенции и статьей 13 Конвенции, является явно необоснованной по смыслу подпункта «а» пункта 3 статьи 35 Конвенции;

В СВЯЗИ С ЭТИМ ПРОШУ:

отклонить жалобу Подчасова А.В. на предполагаемое нарушение его прав, гарантированных статьей 8 Конвенции и статьей 13 Конвенции, в соответствии с подпунктом «а» пункта 3 и пунктом 4 статьи 35 Конвенции.

М.В. Виноградов